

Exam : GREM

**Title : GIAC Reverse Engineering
Malware**

Version : DEMO

1.Which outcome indicates successful deobfuscation of malicious JavaScript?

- A. The script is shorter than the original.
- B. The script's original logic and function calls are understandable.
- C. The script no longer executes in any browser.
- D. The script shows increased use of clear text strings.

Answer: B

2.Which of the following dynamic analysis tools is used to trace and debug malware execution?

- A. IDA Pro
- B. OllyDbg
- C. PEiD
- D. CFF Explorer

Answer: B

3.What is the purpose of analyzing embedded scripts in a PDF file?

- A. To enhance the visual presentation of the PDF
- B. To identify potentially malicious code
- C. To correct typos in the PDF text
- D. To improve the compression of the PDF file

Answer: B

4.Why is it important to analyze the control words within an RTF document when investigating for malicious content?

- A. To identify custom styles applied to the document
- B. To detect hidden instructions or shellcode
- C. To understand the document's layout structure
- D. To verify the document's compatibility with different viewers

Answer: B

5.Which of the following is a potential indicator that an Office macro is attempting to download additional payloads?

- A. Interaction with a local database.
- B. Execution of complex mathematical calculations.
- C. Use of system networking commands.
- D. Modification of document metadata.

Answer: C